可信云服务

丁 滟[1)] 王怀民[2)] 史佩昌[1)] 吴庆波[1)] 戴华东[1)] 富弘毅[1)]

[1)](国防科学技术大学计算机学院 长沙 410073)

[2)](国防科学技术大学并行与分布处理国家重点实验室 长沙 410073)

摘 要 云服务是一类依托于云计算平台的新兴网络服务,其外包服务模式以及云平台自身的安全风险引起了用户的信任问题.云服务可信与否成为用户业务向云迁移的最大顾虑.如何构建安全可信的云服务,成为近年来研究领域的热点之一.该文在分析云计算安全威胁的基础上,提出了可信云服务的定义,并从用户信任预期、安全威胁来源和技术针对的安全目标等角度对可信云服务研究技术的类型进行了划分;然后,系统地梳理了数据存储外包、计算外包、虚拟机外包等典型云服务的安全可信研究工作;最后,探讨了可信云服务的未来研究趋势.

关键词 可信云服务;数据存储外包可信;计算外包可信;虚拟机外包可信

中图法分类号 TP311 **DOI 号** 10.3724/SP.J.1016.2015.00133

Trusted Cloud Service

DING Yan[1)] WANG Huai-Min[2)] SHI Pei-Chang[1)] WU Qing-Bo[1)] DAI Hua-Dong[1)] FU Hong-Yi[1)]

[1)](*School of Computer Science, National University of Defense Technology, Changsha* 410073)

[2)](*National Laboratory for Parallel and Distributed Processing, National University of Defense Technology, Changsha* 410073)

Abstract Cloud service is a kind of emerging network service mode built on the platform of cloud computing. Its outsourcing feature and the security risks with the platform both introduce the trust problem, which becomes the largest misgiving when the users make decision to move their business onto the cloud platform. So the study on achieving trusted cloud service has become one of the key focuses in the research field. In this paper, the definition of trusted cloud service is proposed on the basis of analysis on the security challenge of cloud computing. Taxonomies of trusted cloud service are introduced respectively from the views of trust anticipation of the user, the source of security threat and the security objective of the technique. Then the techniques concerning trusted outsourcing of data storage, computation and virtue machine are analyzed systematically. In the end, the future research trend in this area is presumed.

Keywords trusted cloud service; trusted data storage outsourcing; trusted computation outsourcing; trusted virtue machine outsourcing

1 引 言

随着云计算技术的成熟,以 Amazon EC2、Google App Engine 等为代表的云服务得到蓬勃发展,越来越多的企业和个人通过外包服务来降低计算成本.IT 资源服务化的思想日益普及,呈现“一切皆服务”(X as a Service, XaaS)的趋势,服务成为云计算的

收稿日期:2013-08-20;最终修改稿收到日期:2014-09-03.本课题得到国家“九七三”重点基础研究发展规划项目基金(2011CB302600)和国家自然科学基金(61161160565)资助.**丁 滟**,女,1977 年生,博士,助理研究员,中国计算机学会(CCF)学生会员,主要研究方向为信息安全、操作系统与分布式计算.E-mail: dingyan.nudt@gmail.com. **王怀民**,男,1962 年生,博士,教授,博士生导师,中国计算机学会(CCF)理事,主要研究领域为分布式计算、信息安全和软件工程. **史佩昌**,男,1981 年生,博士,助理研究员,主要研究方向为信息安全、云计算、内容分发网. **吴庆波**,男,1969 年生,博士,研究员,主要研究领域为基础软件、操作系统. **戴华东**,男,1975 年生,博士,研究员,主要研究领域为基础软件、操作系统. **富弘毅**,男,1978 年生,博士,工程师,主要研究方向为高性能计算、并行计算、并行编译与容错.

核心概念.然而,在云计算带来便利的同时,服务资源的集中化也进一步增加了安全防范的难度,云服务的安全问题日益凸显.早在2007年就有报道称著名的云服务提供商Saleforce.com因为在服务过程中受到安全攻击而造成大量的租户数据信息泄露或遗失;2010年谷歌公司的两名员工由于入侵云平台租户的账户并获取隐私数据而被解雇.云计算环境所受到的安全威胁严重地影响了用户对云服务提供商的信任程度.2010年富士通公司的调查表明,88%的潜在用户对云的可信性问题表示十分关注与担忧.而RSA首席技术官Hartman也指出:在企业将当前应用向第三方云环境迁移的过程中,首先需要考虑的就是对云服务的信任问题.因此,云服务能否被顺利地推广和使用,在很大程度上取决于云服务的可信性能否达到用户满意的程度.

由于云服务的"外包"特性,用户对云提供商是否能够对其数据安全提供保障,对其应用程序是否按照约定的方式安全执行产生了怀疑,亦即云服务的可信性问题.云服务的可信问题不仅指服务计算环境受其开放、共享等特点而导致服务的客观安全性上受到威胁,同时还指服务质量与服务结果可能受云服务提供商的主观意志等因素导致的不可信.为了规范云服务提供商的行为,帮助用户选择可信的云服务,目前,多家安全标准组织公布了云服务的安全标准,其中,规模最大的云安全标准组织云安全联盟(Cloud Security Alliance,CSA)发布了《云控制矩阵(Cloud Control Matrix,CCM)》等多部安全标准,内容涉及十多个云基础设施领域,不仅涵盖云服务本身的安全问题,还包含了政府、法律法规和硬件架构等合规解决措施,得到业界较广泛的认可.此外,美国国家标准与技术研究院(NIST)、电气和电子工程师协会(IEEE)以及欧洲网络与信息安全局(ENISA)都颁布了自己的云安全标准,分别在公有云计算安全和隐私、云供应商之间的互操作性以及云合同安全服务水平监测等方面为用户提供指南.尽管目前很多业内的云服务提供商还未采用统一的标准,而是各自采纳了自己所认可的准则,但随着云产业的不断演变与架构调整,最终会形成云服务供应商公认的认证标准.云用户可以通过贯彻与广泛采用这类标准对云服务提供商进行安全评估.

在学术界,针对云服务安全可信的研究涵盖了系统安全、数据安全及隐私保护、计算验证等各个方面,具体的研究涉及到系统架构、密码学、计算理论等多个层面.从2009年开始,在OSDI、SOSP、S&P、CCS、INFOCOM等各大安全、系统以及网络方向的顶级会议上,云计算安全以及服务可信技术都是持续热点,CCS专门设置了关于云计算安全的研讨会.著名的信息安全国际会议RSA大会也连续多年将这一问题列为焦点议题.为了更好地把握国际主流的研究方向与先进技术,本文对当前研究热点的云服务可信技术研究进行分析总结,以期为研究人员精准、实时地把握最新研究动态和未来研究趋势提供借鉴.

本文第2节首先对云计算技术带来的新的安全威胁进行分析,提出可信云服务的定义;第3节从用户信任预期、安全威胁来源以及技术的安全目标3个方面,对当前可信云服务的研究技术进行分类;第4节针对目前关注最多的数据存储外包、计算外包以及虚拟机外包等服务在可信研究方面的关键技术进行总结与比较;第5节对可信云服务的未来研究趋势进行分析和展望;最后总结全文.

2 可信云服务基本概念

2.1 云计算的定义与特性

NIST对云计算的定义为①:云计算是一种通过互联网可以随时随地、便捷、按需地访问共享资源池(如计算设施、存储设施、应用服务等)的计算模式.伯克利对云计算的定义为[1]:云计算既指通过互联网以服务方式提供的应用程序,也指在数据中心用来提供这些服务的硬件和系统软件.综上所述,云计算的核心思想是资源的服务化与用户的广泛性.软硬件资源均可以以服务的形式进行访问,并且用户通过互联网就可以简单地接入使用服务.具体来说,云计算包括5个特性①:

(1)按需服务.可以根据用户的需求对服务资源进行自动分配,而不需要服务管理员干预.

(2)泛在接入.用户可以利用各种标准终端(如智能手机、平板电脑、笔记本等)通过互联网访问云服务.

(3)资源池化.服务资源以资源池的方式,利用虚拟化等技术,根据用户需求以多租户的形式服务.资源的放置、管理与分配策略对用户透明.

(4)快速伸缩.服务的规模可以根据用户需求情况快速伸缩,以自动适应业务负载的动态变化.

① The nist definition of cloud computing[EB/OL]. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, 2011

(5)按使用收费.云服务的资源使用量可以被监控,并依据资源使用情况对服务计费.

2.2　云计算环境下新的安全威胁

在大型主机时代,主要服务特点是计算资源在企业内部集中部署,统一管理.系统的管理维护者拥有对计算环境的全部控制权.主机的用户大都采用终端模式与主机相连,本地不进行数据处理与存储.此种计算模式下,安全威胁主要来自于系统外部,安全研究的目标主要是防护来自系统外部的攻击,具体技术包括用户身份认证、访问控制等系统安全研究以及防火墙保护、病毒防范等网络安全研究等.

与此相对,云计算可以被看作是以数据中心为核心的"集中计算",其服务模式呈现"对外集中,对内分布"的特点.从用户的角度,服务的提供方是单一的主体,用户的服务请求由云服务方进行集中处理;而在云服务的内部,则由数据中心的分布式计算资源来协同完成服务过程.云计算内部复杂的资源共享方式与服务处理模式,以及通过互联网的泛在访问,大大增加了云计算安全防护的难度.同时,云计算外包服务的特性也使用户丧失了资源的独占性与一定程度的数据私密性,并且云计算的按使用收费的特性也为服务方为追求利益而损失服务质量埋下隐患.根据云计算的特性,云计算的模式带来如下安全威胁:

安全威胁 1. 外包服务模式带来数据安全与服务信任问题.

云计算外包的服务模式使用户的数据管理与计算等都在云上完成,用户主要关心应用的处理逻辑而无需关心底层细节,但由此,用户将对数据与处理的控制权也交由云服务方来控制,云上的数据及处理是否安全可控成为需要关心的问题.

安全威胁 2. 资源的共享使用带来安全隔离问题.

云计算使用共享资源池来提供用户所需的资源,采用虚拟化技术与物理资源相结合的方式分配资源,不同用户的资源在逻辑视图上相互独立,但其底层物理映射却有可能共享相同的物理资源.恶意用户可能通过各种攻击手段,获取其他用户的信息.

安全威胁 3. 服务的多级模式带来统一安全监控问题.

云计算为用户提供的服务可能处于系统结构中的不同层级,并且位于上层的服务可以基于下层服务来构建.例如,基于基础架构级(IaaS)的服务上构建平台级服务(PaaS),在其上再构建软件级服务(SaaS).传统的安全监控主要集中在单一级别,在多级云服务的架构下,就必须将各级监控技术组合,才能完成针对云计算的统一视图的系统安全监控.

安全威胁 4. 效用计算模式带来服务可信性度量与计费问题.

云计算的"pay-as-you-go"模式使得服务根据使用情况来进行收费,而追求商业利益是商人的天性,不可避免地会出现某些服务商为了追求商业利益而对服务作假.资源使用计量是否真实可信,是保证按使用付费的准确性的前提.

综上所述,用户对云服务的安全怀疑主要集中在客观与主观两个方面:在客观方面,云计算的集中服务模式使其更容易成为安全攻击的目标,而云计算的大规模分布式处理也大大增加了安全管理的难度,因此,服务商是否具有足够的安全管理能力来保护用户信息安全值得怀疑;在主观方面,由于云计算模式下,用户信息的存储、管理以及应用处理都在云服务方完成,用户丧失了控制权,此时如何保证服务方忠实履行自己的服务协议,保证服务质量,并且不会通过自己的特权来违规使用用户资源获利成为必须要解决的问题.

2.3　可信云服务的定义

文献[2]中将云服务定义为"所有在远端部署并通过 Internet 或私有网络访问的应用与服务的总称",涵盖了各种形式的网络服务.其中,以云平台为底层支撑的新兴服务在利用云计算提供各种便利的同时,还要面对各种新产生的安全威胁,因此,成为可信云服务研究的主要研究对象.

可信系统的概念由 Anderson 于 20 世纪 70 年代初首次提出,之后数十年,计算系统的可信性问题就一直被广泛关注,人们尝试从不同的角度对系统的可信性的概念进行阐述.在云计算环境下,如何评价一个服务是可信的服务,成为用户选择云服务的重要评价标准.下面,给出可信云服务的定义.

定义 1.　如果云服务的行为和结果总是与用户预期的行为和结果一致,那么就可以说云服务是可信的.

这里,我们主要针对云服务在安全性方面的服务质量来考虑服务的可信性.根据上述定义,可以看出,要讨论云服务的可信性,需要明确以下 3 个方面的问题:

(1)用户的界定.不同的用户拥有的信息安全敏感度不同,从而对云的安全性认定也不同.例如,热点人物的信息敏感度高,外包至云上存储容易导致恶意者的攻击,泄露隐私或破坏其数据安全;而普

通用户信息敏感度较低,将其外包至云上存储则更多地突出了信息保存不易失等特点.

(2)服务行为的区分.不同类型的服务可能涉及到的可信问题也不同.如果在云上运行的是开放性的服务,如网站、社区等,服务的主旨是希望更多的用户访问,云的便利性使其更具竞争力;但如果是公司内部的业务,服务对象、流程、结果等各个环节都可能涉及公司的机密,这样的业务迁移到云上,对服务环境的安全要求就会很高.

(3)信任预期的度量.不同用户针对不同类型的服务,其安全诉求也不同.与自己信任预期相对应的服务对用户来说就是可信的服务.在具体使用过程中,用户可以首先衡量服务的可信度,然后选择能够满足自己信任需求的服务.

3 可信云服务技术分类模型

云计算环境中,服务通过广域网面向用户开放.这种服务模式使得服务必须面对来自广域网的各类安全威胁,并且在云服务内部的各类新兴技术也将面临安全的考验.因此,各类针对云服务的可信性研究成为热点.

如图 1 所示,下面将从用户信任预期、安全威胁来源以及安全技术实现的安全目标 3 个维度来对可信云服务技术进行分类.

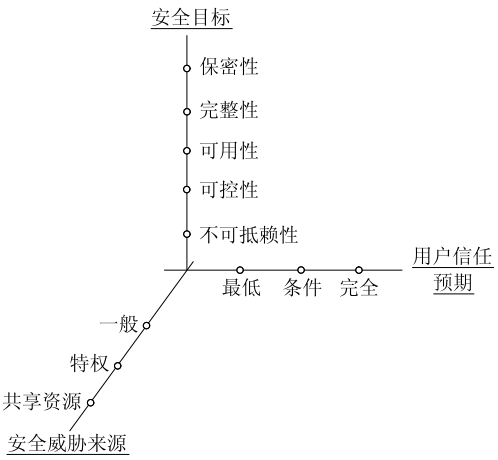

图 1 可信云服务技术分类模型

3.1 按照用户信任预期分类

针对可信云服务的研究,可以根据用户对云服务的信任预期的不同分为 3 个类别:

(1)完全信任(Trust Everything)

用户完全信任云服务方会负责保护用户的利益.此种假设下,服务是否可信主要取决于云服务方是否能够具有足够的能力保障系统的安全性,维护用户利益不被侵犯.例如,针对虚拟计算环境的安全隔离、完整性检验等方面的研究多基于这一类前提假设.

(2)条件信任(Trust Something)

用户对云服务方有所怀疑,但是信任经过某种手段验证的云服务,例如,通过具有资质的第三方检验的服务或者利用可信计算技术中 TPM 芯片等硬件手段验证过的服务等.

(3)最低信任(Trust Nothing)

用户怀疑云服务方的动机与能力,因此对服务方的信任为最低水平,仅信任服务的可用性、性能、容错等最低保障,其余安全问题靠用户自己解决.当前针对数据存储以及计算验证等方面的问题多属于这一类研究.

可以看出,上述条件信任与最低信任中,用户对云服务方都是持怀疑态度的.honest-but-curious 是当前对云服务的一种主流假设,认为服务方基本会提供诚实的服务,但仍需采取谨慎态度.随着云计算技术的发展,对云服务质量监管将成为对云服务可信评价的重要手段,一般情况下,由具有可信资质的第三方来完成.能否通过第三方的检验认证将成为衡量云服务是否可信的重要标准.为了使第三方完成监督检验,云服务需要在云端的服务处理机制中向第三方提供检查接口,由第三方来具体实施检验,得出检验结果.然而,要实现第三方监管,除了技术上的支持,还需要相应的规范条文,以及对第三方的资质认证等一系列的工作,才能形成统一的监控管理.在一定程度上,要实现这样的监管体系,还需要较长时间的努力.因此,当前情况下,研究用户为主导的服务检验手段具有很强的现实意义.

3.2 按照安全威胁来源分类

根据云服务中存在安全威胁来源的不同,如图 2 所示,可信云服务的研究分别针对以下 3 类安全威胁进行研究.

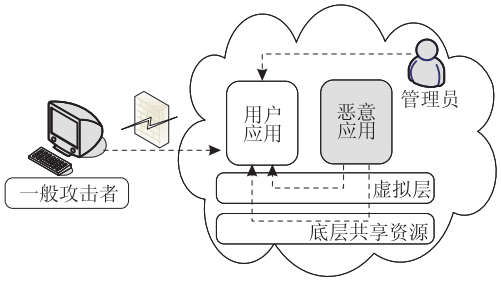

图 2 云服务安全威胁来源

(1)一般安全威胁

指云系统中存在的软硬件漏洞、网络防护能力不足，以及在社会工程学等常规手段攻击下可能造成的安全风险.此种安全威胁并非仅存在于云服务中，而是在一般信息系统中就早已存在的固有安全问题.但是，由于云计算平台的开放性，使服务的安全边界难以判定，并且云服务的集中化处理也必将吸引更多的恶意攻击，因此，云服务系统必须具备很高的一般安全威胁防范能力.

(2)特权安全威胁

特权安全威胁是由云服务的外包特性产生的.由于云服务的数据存储以及处理等全部在云平台上完成，用户失去了对自己数据以及计算的控制权.此时，如果云平台的管理员具有恶意，就可以利用自己的特权随意访问与修改用户的信息，或者为用户提供错误的计算结果.Gartner 的云安全报告中指出，云平台的最大的安全威胁来自于平台提供商对于租户隐私数据的非法访问.因此，在可信云服务的研究中，如何针对特权用户的安全攻击行为进行防范与补救，也成为研究的一个重点.

(3)共享资源安全威胁

云服务的另一个重要特点是资源的共享，通过虚拟化技术的支持，不同用户的应用在同一计算平台上运行，共享物理设备.因此，云服务的恶意用户可能通过底层平台的漏洞对同一物理平台上的其他用户进行旁路(Side Channel)攻击.虚拟机的安全隔离必须能够抵御此类攻击，才能保证用户的信息安全.

简而言之，外部攻击者主要利用一般安全威胁，通过常规攻击手段对云服务进行攻击；特权安全威胁则主要来自于云服务的内部工作人员，甚至是云服务提供商本身，利用自身特权破坏用户的信息安全；而共享资源安全威胁主要来自于云服务的用户之间，利用底层的共享资源发起攻击.在云计算模式下的新的安全威胁中，外包服务模式带来的数据安全、服务验证以及可信计费等问题，主要都是对服务方的服务行为是否规范的怀疑，因此属于特权威胁；而计算资源的安全隔离等问题则主要关注在云计算环境中的计算资源共享而导致的威胁，属于共享资源威胁.在可信云服务的研究中，不仅要应用已有的安全防护手段抵御一般安全威胁，更重要的是针对云服务所特有的安全威胁形式进行研究，防护来自于服务方与共享资源用户之间的攻击行为.

3.3　按照安全目标分类

可信云服务技术分别针对云服务系统中不同的安全问题，围绕不同的安全目标进行研究，其中，核心的安全目标包括保密性、完整性、可用性、可控性和不可抵赖性 5 种特性目标：

(1)保密性(Confidentiality).指信息只有被相应授权的主体才能够获取.这里既包括数据信息的内容不被非授权主体获得，还包括用户的行为等隐私的保密.

(2)完整性(Integrity).指信息不能够被未经授权的主体篡改，使信息保持其真实性.这里既包括存储的数据不被恶意修改，也包括数据处理等服务结果不被恶意篡改.

(3)可用性(Usability).指被授权的主体在需要使用服务时能及时访问服务的能力.可用性是在网络化服务必须满足的一项基本的信息安全要求.

(4)可控性(Controlability).指对信息系统中的信息和系统行为实施安全管理与监控，防止对信息和信息系统的非法滥用.

(5)不可抵赖性(Non-repudiation).原指信息交换过程中的行为不可抵赖，也可以扩充到信息系统中的行为人不能否认自己的处理行为.可审计性(Audiability)与可鉴别性(Authenticity)均与此类似，可审计性更侧重于对系统行为的记录，可鉴别性则侧重于行为主体的身份的真实性.

针对上述安全目标，可以采取的安全手段可以分为主动控制与事后追责两类.主动控制类的技术如隐私保护、安全隔离等在处理的过程中进行控制，使威胁系统安全性的行为无法发生；而事后追责的技术主要通过对处理过程的信息进行记录与分析，从而发现恶意行为，完整性验证、安全审计等属于事后追责技术.事后追责的技术虽然不能直接地控制恶意行为的发生，但由于安全手段的存在意味着违规的行为将会受到惩罚，从而形成一定的威慑作用，可以间接地避免恶意行为.

下面，就以上述提出的可信云计算计数分类模型为基础，对当前可信云服务研究的焦点技术进行分析.

4　关键技术研究

云服务主要以外包的形式，利用云计算平台的支持，为用户提供从底层计算环境到上层应用的多样性的服务.由于云服务的外包特性，服务的信息存储与处理都在云端完成，用户无法具体掌握服务的执行情况，此时，服务信息有没有被泄露、服务是否

确实按照用户的意图来执行等等问题都会造成用户的忧虑.因此,尽管具体服务类型的差异导致各类服务可信性需求的表现形式各有不同,但总体来讲,当前的可信云服务研究的目标主要集中于服务的保密性与完整性两个方面.

服务的保密性主要指服务涉及的信息只被具有相应权限的主体所掌握.不同的服务要求保密的信息对象不同,但综合来说,主要可以分为数据保密性与行为保密性两个方面:(1)对于数据的保密,主要通过密码学来保护,同时还要考虑对经过保护的数据能否进行安全便捷的访问.其中,基于属性的密码算法在加密数据的同时还为后续对这些数据的访问控制提供支持;密文数据检索技术则对加密后的数据提供检索支持,方便用户对数据的查找与定位.而当外包的数据还要在云端进行计算时,全同态加密技术针对一般计算问题,从理论上解决了密文数据参与计算后的计算结果还原问题;而对于具体的数学问题,则可以设计相应的数学变换方法来保护输入数据以及结果的保密性;(2)对于行为的保密性,主要是保护服务的具体操作行为不被非授权主体获取与破坏.例如,在虚拟机外包服务中,虚拟机一旦指定为某个用户提供服务,那么该用户在虚拟机中的行为就应该对管理员以及其他用户严格保密.目前主要采用 Hypervisor 监控技术等对虚拟机安全进行监控与保护.此外,基于旁路攻击的研究则针对虚拟机间的非系统逻辑漏洞研究隔离与防护机制.

服务的完整性主要指服务是按照用户意图真实执行的,而不是提供一个虚假的服务结果来欺骗用户.针对不同服务形式,完整性要求的侧重点各有不同:存储服务的完整性主要是数据在云端不被篡改,目前的数据完整性保护机制主要有数据持有性与可恢复性验证等审计手段,通过少量的标志性数据的存储完整性来评估整体数据集的存储状态,并对文件内容进行恢复;而对于以计算为服务内容的外包计算云服务,服务所得到的计算结果是否是按照用户要求真实计算完成的就成为完整性验证的目标.目前,交互式证明系统、概率可验证明系统等可验证计算理论研究都围绕外包计算云服务的新特性,形成新一轮研究热点.而针对实际应用问题,以大规模线性计算、海量数据处理为代表的计算结果验证研究也进一步展开;在系统底层,虚拟机的执行验证成为研究重点,目前通过可信计算等技术,对虚拟机的行为进行验证,控制虚拟机按照用户的要求执行.

目前的服务可信性研究技术主要集中在数据存储、大规模计算以及基础计算环境(即虚拟机)的外包服务中的安全可信问题.下面,就对这 3 类服务的可信技术进行分析与总结.

4.1 可信数据存储外包

数据外包至云上存储,使对数据的控制权从用户转移到了服务方.此时,要求云存储服务满足两个基本的安全目标:机密性与完整性.

数据机密性主要指数据的内容只能被数据拥有者授权的用户才能访问,其他用户以及服务的提供者都无权访问数据.由于数据保存在服务方,用户无法获取服务方对数据的使用情况,因此,主要依靠密码学的方法来保护数据的机密性:用户首先对数据加密,然后以密文形式保存在云服务方.为了防止服务方在访问控制决策中的欺骗问题,对数据的访问控制也主要通过密码学来完成.

数据完整性主要指服务方对用户数据的任何未经授权的修改都能被用户发现.传统的完整性保护方法主要通过基于密码学的校验机制等,但由于云存储的数据量巨大,很难对所有数据计算校验和,因此针对云存储的数据完整性多基于零知识证明或概率验证的手段,对部分存储数据进行取证,以高置信度来保证数据存储的完整性.

此外,由于云上的数据主要以密文形式存储,在数据的利用方面,如何检索密文信息成为重要的研究问题.

4.1.1 数据确定删除

云计算环境下,为了保护用户的数据隐私不被泄漏,数据往往以加密的形式保存在云上.然而,当用户要求对文件进行删除时,云服务方可能并未完全移除数据的所有副本,一旦数据的密钥不幸被泄露,或者随着时间推移,服务方获得更强的解密能力或更多的相关信息时,数据隐私的泄露则成为可能.因此,需要通过技术手段来保证存储在服务方的数据确定被删除.

为了解决存储在服务方的数据确定删除(Data Assured Delete)问题,Perlman[3] 提出了基于时间的文件确定删除技术,对文件使用 data key 加密,然后再使用由独立的密钥管理服务管理的 control key 对 data key 进行加密.由于 control key 仅具有一定的有效期,当时间超期以后,control key 将被删除,从而使得 data key 以及文件内容都无法被解密.在此基础上,Geambasu 等人[4] 实现了基于时间的文件确定删除原型系统 Vanish,将秘密共享技术与大规模的广域分布式 Hash 表(Distributed Hash

Table，DHT）相结合，通过 DHT 的动态性来实现一定期限后的数据确定删除. 在对数据进行加密封装时，首先使用随机的数据密钥 K 加密，然后利用门限秘密共享（threshold secret sharing）技术将 K 分割为 N 个片，保存在 DHT 的 N 个节点中，用户在解密时只需获得其中 m 个分片即可对数据进行解密. 为了实现更细粒度的确定删除，Tang 等人[5]设计实现了基于策略的文件确定删除存储系统 FADE（File Assured Deletion）. 系统为文件关联一个原子文件访问策略，每个原子策略对应一个 control key，所有 control key 由密钥管理者进行管理. 加密文件使用的 data key 由策略对应的 control key 进行加密，如果某个 control key 被作废，则相应的 data key 与文件内容均无法解密，从而达到安全删除. 王丽娜等人[6]根据云存储的海量数据特性，提出了一种适于云存储系统的数据确定性删除方法. 该方法首先通过密钥派生树组织管理密钥，然后利用秘密共享以及 DHT 网络实现密钥的定期删除，有效解决云存储中海量数据造成的密钥管理难题.

4.1.2　数据可恢复证明与数据持有证明

在云存储的环境中，用户如何判断数据的完整性成为难题. 由于数据存储规模巨大，用户不可能将数据下载后再验证其正确性，因此，数据可恢复证明与数据持有证明主要研究如何在取回很少数据的情况下，以高置信概率判断远端存储的数据是否满足完整性要求.

数据可恢复证明[7]（Proof-of-Retrievability，POR）由 RSA 实验室的 Juels 与 Kaliski 首先提出，该方法基于零知识证明的思想，由存储服务方（证明者）向用户（验证者）提供证据证明其文件被完整地保存，用户可以恢复出完整的文件. 在该方法中，证明者与验证者都不需要了解整个文件的内容，符合云存储服务中数据海量分布式存储的特点；Shacham 等人[8]针对 Juels-Kaliski 模型中任意对手的威胁模型设计了提供完全证明的 POR 机制，并利用同态加密的特性减小验证交互信息的长度；Dodis 等人[9]对 POR 问题的使用边界等特性进行了更深入的分析与讨论，并针对不同的特性设计接近最优的 POR 机制. 数据持有证明（Provable Data Possession，PDP）由 Ateniese 等人[10]提出，通过概率分析的手段对外包至云上存储的数据随机采样，生成数据持有性相关证据，由用户保留. 在验证阶段，用户使用元数据向服务方发起挑战，通过查询这些数据是否在服务方正确存储来以一定的置信度证明服务方是否正确持有数据. 由于 PDP 机制主要针对静态存储的数据，Erway 等人[11]设计了动态数据持有证明（DPDP）框架，支持对存储数据的可证明的动态修改. Curtmola 等人[12]则针对云存储系统中普遍使用的多副本存储技术，提出了多副本 PDP 验证方法 MR-PDP.

4.1.3　可信访问控制

外包存储的数据以密文形式保存在服务方，数据拥有者在将云上的数据共享给其他用户时，希望能够对这些用户的访问行为加以控制，例如对个人健康数据的共享时，来自不同机构的用户对数据具有的访问权限也不同[13]. 由于无法信赖服务商是否忠实地实施了用户定义的访问控制策略，因此，现有研究通过非传统访问控制类手段实施数据对象的访问控制.

基于属性的加密（Attribute-Based Encryption，ABE）机制为对加密数据的访问提供了一种基于密码学的控制途径. 该机制允许数据的拥有者根据属性对数据进行加密，只有符合密文属性要求的用户才能解密消息，从而在区分用户群体的基础上保证数据机密性，达到对数据进行访问控制的目的[14]. 最初提出的基本 ABE 机制[14]仅能支持门限访问控制策略. 为了表示更灵活的访问控制策略，学者们进一步提出密钥-策略 ABE（KP-ABE）[15]和密文-策略 ABE（CP-ABE）[15]两类 ABE 机制.

在将 ABE 应用到云存储的访问控制上时，考虑到数据拥有者的计算能力有限，Yu 等人[16]将 KP-ABE 机制与基于代理的重加密机制相结合，提出了细粒度可扩展的云存储访问控制机制，允许拥有者将访问控制决策以及密钥属性更新所带来的大部分计算开销分布到云上完成，在不损失数据机密性的前提下，大大降低了访问控制机制给数据拥有者带来的计算开销. 孙国梓等人[17]提出一种基于 CP-ABE 算法的密文访问控制机制，并从访问权限控制及访问控制体系结构两个方面进行研究. 洪澄等人[18]则重点解决访问控制策略的动态性带来的数据重加密问题，在基于属性的加密基础上提出了基于秘密共享的密文访问控制方法 HCRE（Hybrid Cloud Re-encryption），将重加密过程转移到云端执行，从而降低权限管理复杂度，实现高效的动态密文访问控制.

4.1.4　密文检索

云计算环境下，数据以密文形式存储在云上，如何对这些密文数据进行搜索，发现用户想要的信息

成为必须要解决的问题.传统的可搜索加密技术允许用户将密文数据作为文档,根据关键字进行搜索,以获得感兴趣的内容,主要分为对称可搜索加密(Symmetric Searchable Encryption,SSE)机制、基于公钥加密的非对称的可搜索加密(Asymmetric Searchable Encryption)等,但这些技术主要基于密码原语开发,将其应用于云中的大规模数据的高层检索时,将极大程度地影响系统的可用性.

为了实现更加灵活易用的检索功能,使搜索任务能够适应现实世界的搜索需求,学者们提出了对密文数据的合取关键字搜索(Conjunctive keyword search)[19],允许用户对搜索任务定义多个关键字,搜索结果遵循"all-or-nothing"原则,只返回满足所有关键字的结果.合取关键字搜索技术的密码原语机制带来很大的计算或通信代价.为了更进一步增加检索的灵活性,出现了谓词加密机制(Predicate encryption)[20],支持关键字的合取与析取搜索,可以潜在地支持任意的查询类型,包括 CNF/DNF 范式,但是需要指数级的复杂度.此外,为了增加搜索结果的准确性,分级搜索(ranked search)技术对搜索结果进行排序,总是返回与关键字相关度最高的结果,降低了网络开销,更符合云计算 pay-as-you-go 的特征.为了更贴近明文检索的用户使用习惯,Wang 等人[21]提出了基于相似度的检索,通过对给定的文档集合构建相似度关键字集合,为用户实现更为高效的检索机制.

以上的搜索技术主要针对数据的机密性进行保护,同时,在搜索的过程中,用户所使用的关键字、转换成的陷门(trapdoor)以及搜索的结果都涉及到用户的隐私.因此,在利用加密机制保护数据机密性的基础上,对数据的搜索行为的隐私保护也产生了一系列研究,分别针对基于公钥机制的谓词隐私[22]、多关键字分级检索[23]、相似度关键字检索[21]等方面进行搜索行为隐私保护,并且结合实际的应用案例,研究层次式授权搜索能力[24]以及图结构数据搜索[25]等实际问题中涉及的隐私保护问题.

4.1.5 分析与小结

云存储是当前的热点云服务.用户的数据保存在云上,各项研究致力于保证云上存储信息的机密性、完整性以及对数据的可信利用.下面,对上述技术进行总结,具体总结如表 1 所示.

针对云存储的数据安全的研究主要分为数据存储的安全以及在此基础上如何对数据加以利用两个方面.用户对云服务方是否会利用特权来获取数据信息或破坏数据完整性成为最大的怀疑,因此,对云服务的信任预期为最低预期,用户自主采用数据加密来保护数据信息安全,并且在设计密码算法时重点考虑加密数据的利用,保证这些数据在被使用的过程中不会造成信息的泄露,并且要保证服务方真实可靠地按照用户的意愿执行.

表 1 可信数据存储外包技术比较

安全问题	主要技术	用户信任预期	安全威胁来源	安全目标			
				保密性	完整性	可控性	可用性
数据静态存储	数据确定删除	最低	特权	√			
	POR & PDP				√		
数据动态利用	可信访问控制			√		√	
	密文检索			√			√

然而,可信云存储研究仍存在不足.目前,云存储服务的数据机密性研究主要针对静态存储数据,采用加密等方法进行隐私保护,数据在云上仅作为档案来保管,并不参与其他的计算.但是随着云服务的一体化架构逐步形成,很多位于上层的云服务可能直接使用云存储的数据进行计算.这样,在设计数据存储机密性保护方案时,还需要考虑该数据在应用中是否能够参与计算,并且在计算过程中不泄露数据隐私.静态数据隐私保护技术在解决数据的动态应用隐私问题方面存在不足,因此,针对动态数据的隐私保护还需要进一步研究.

4.2 可信计算外包

在云计算环境中,用户的计算任务被外包至云上完成.这一过程可能带来两个问题,首先,具体的计算过程用户不可控,而由于服务方追求商业利益等原因,导致计算结果的可信性低.由于用户的计算能力往往较弱,如何使用户能够对服务方反馈的计算结果进行验证,是保证计算完整性的关键;其次,外包至云上计算的任务可能涉及到敏感的数据,例如国家机密数据、商业机密以及受各种法规保护的个人信息等,如何在对这些数据操作的同时保护数据的隐私,成为必须要解决的问题.因此,针对可信计算外包的工作主要分为了计算验证与隐私保护两个方面,在计算理论、具体科学计算问题以及计算机制等各个层面均有研究.下面,就分别从这几个层面介绍当前的研究工作.

4.2.1 计算理论研究

在计算复杂性研究领域,对于计算外包的可信验证问题主要集中于解决对于任意函数的计算验证.交互式证明系统中,通过验证者(Verifier)与证明者(Prover)的博弈过程,使验证者能够判断证明

者是否正确完成了计算.这类问题一般假设验证者具有多项式时间确定性图灵机计算能力,而证明者则具有无限大的计算能力.概率可验证明(Probabilistically Checkable Proofs,PCP)系统中,证明者仅需向验证者提供一个证据,由验证者在其中随机验证,但可能导致 PCP 系统的证据长度超出验证者的处理能力.最近,Goldwasser 等人[26]提出的证明系统可以在接近线性时间内验证任意的多项式时间的计算,降低了系统验证开销.由于 PCP 系统的性能开销巨大,实现困难,Setty 等人[27]则实现了基于 PCP 的论证系统 PEPPER,通过对该系统的设计、实现以及评价工作,说明基于 PCP 系统也可以以较小的性能代价在实际系统中实现.为进一步减小验证开销,Cormode 等人[28]针对数据流提出证明系统,该系统中验证者无需保存问题相关的所有输入,而是将数据按照上传顺序等拆分成数据流,通过数据流的变化,动态地验证证明者的计算是否存在错算或漏算,该方法验证者方的存储开销与通信开销为对数级开销.

由于外包计算的内容可能涉及到用户的隐私,因此完成计算的同时必须保护隐私.同态加密(homomorphic encryption)允许证明者以密文的形式完成计算,从而防止用户的数据隐私泄露.Gentry[29]最近的工作成果:基于理想格的全同态加密使得理论研究向实际的应用更近一步.Chung 等人[30]基于全同态加密机制设计了安全的外包计算验证机制,将验证的开销分为在线开销与离线开销两个阶段,将大部分的验证开销分布在离线阶段,从而换取在线操作的高效完成;Gennaro 等人[31]则在此基础上,在外包计算之前对数据进行预处理,通过将加密电路(garbled circuit)与全同态技术相结合,在完成对计算结果验证的同时,还实现了对输入数据及结果的隐私保护目的.

4.2.2　大规模线性计算

由于同态加密系统尚处于理论研究阶段,因此在实际应用中,学者们往往从具体的计算问题入手,研究针对具体问题的计算外包的计算验证以及隐私保护问题.

在大规模线性计算中,针对一般线性计算、线性方程组、以及线性规划的安全外包工作中,都将结果验证作为安全外包的考虑内容之一,利用线性计算的特点,针对服务方反馈的结果进行验证.并且,通过数学变换等技术,保护用户计算数据的隐私不会泄露.Atallah 等人[32]对大规模的线性代数计算外包进行研究,通过矩阵变换等方法,以矩阵乘为例设计安全外包计算模式,有效保护计算的隐私并抵御结果欺骗.该方法可以有效抵御多副本验证中的共谋问题,并且不需要加密等开销巨大的操作.Wang 等人[33]在大规模线性方程组的外包求解问题中,利用公钥机制的附加同态属性,允许用户在本地计算一个初始猜想,然后在云上进行逐步的迭代,获取达到近似精度要求的解,以此来保护用户数据的隐私,与此同时,还利用矩阵-向量乘的代数属性,对结果以批处理方式进行验证;在线性规划问题的外包求解中,Wang 等人[34]将线性规划的外包计算分解为公开 LP 求解和私有 LP 参数两个部分,公开的 LP 求解过程在云上完成,私有的 LP 参数则由用户来掌握.该方法首先将 LP 问题的用户私有数据形式化为矩阵与向量的集合,然后通过矩阵乘法、仿射映射等机制将原始 LP 问题进行任意转换,从而保护用户隐私信息.

4.2.3　海量数据处理

在针对 MapReduce 海量数据处理的结果可信性研究中,主要分为内部环境验证和外部计算结果验证两个层面的研究:

在内部节点计算结果验证方面,Wei 等人[35]针对开放式 MapReduce 计算环境中,来自不同资源拥有者的计算节点可能存在的计算结果不可信的问题,提出了基于多副本技术的完整性保护机制 SecureMR,该方法使用多副本的方法对 Map 阶段的工作结果进行验证,只有所有副本的计算结果相同时才能将结果提交至 Reduce 阶段;在此基础上,Wang 等人[36]着重解决多 Map 副本的共谋问题,在计算模型中新引入了 Verifier 角色,对通过多副本验证的计算结果进行抽样复算,一定程度上防止多个副本的共谋欺骗行为;Xiao 等人[37]针对 MapReduce 平台中工作节点可能由于网络攻击等导致的计算结果欺骗问题,设计了一种可记录的 MapReduce 平台,利用可信的审计节点组记录 MapReduce 各阶段产生的结果,通过对各类计算结果的复算验证,发现存在欺骗的工作节点.在对整体计算结果的验证方面,Huang 等人[38]提出了基于水印(watermark)注入的方法来验证用户提交的作业是否被正确完成,在用户提交的作业中事先插入用于验证的水印,在作业结果提交后,验证事先插入的水印作业是否被正确处理,如果水印作业被正确处理,则以一定概率认为整个作业的处理满足完整性要求.

在利用云平台进行数据挖掘的过程中,由于挖

掘的数据集可能涉及用户的隐私,在处理过程中以及结果发布时,如何保护数据的隐私成为云服务需要考虑的问题. Roy 等人[39]设计实现了保护数据隐私的安全 MapReduce 平台 Airavat,该平台在数据处理的过程中利用 SELinux 安全操作系统提供的强制访问控制策略,保护数据分析结果不会在 Map 过程中泄露;在 Reduce 阶段,平台通过统一的可信 Reduce 节点,对分析的结果进行差分隐私(differential privacy)处理,对用户数据的隐私进行保护.

4.2.4 分析与小节

在计算外包的可信性研究方面,主要考虑其计算结果可验证以及对于计算内容的隐私保护两个方面. 当前的研究主要涉及计算理论、具体科学问题以及计算环境等 3 个层次. 表 2 中对这些可信计算外包机制进行对比总结.

表 2 可信计算外包技术比较

计算类型	主要技术	用户信任预期			安全威胁来源	安全目标	
		完全	条件	最低		保密性	完整性
一般计算问题	交互式证明系统		√		特权		√
	基于全同态加密的证明系统			√		√	√
大规模线性计算	数学验证			√			√
	数学变换			√		√	
海量数据处理	MapReduce 验证机制	√		√			√
	Airavat			√	一般	√	

针对一般计算的验证主要为计算理论的交互式证明系统研究,通过验证方与证明方的博弈来证明计算的正确性. 但是理论上的计算证明系统无论从计算复杂性方面考虑,还是基于全同态加密算法的设计,在计算开销以及可适用的计算范围方面都还存在不足,导致这类研究要在实际中应用还有一定距离,需要进一步提高方法的实用性.

而另外的一种外包计算验证的研究思路则针对具体的计算问题,研究计算验证方法. 现有研究已针对在大规模数学计算、海量数据处理等计算类型,通过数据变换、副本验证等技术来对计算结果进行验证. 但是,由于这类研究与要验证的具体问题计算类型相关,不同的计算问题相应的解决方案也不同,因此,在目标问题的多样性方面还需要进一步扩展,针对不同计算问题研究具体的验证方法,因此具有很大的研究空间.

4.3 可信虚拟机外包

基础计算环境——虚拟机(Virtue Machine,VM)的外包服务利用虚拟化技术,为用户提供虚拟的基础计算环境,不同租户的数据与计算可能在相同的物理设备上完成. 虚拟机技术在操作系统与底层硬件之间引入了新的虚拟机监控器(Virtue Machine Monitor,VMM)层,整体计算系统的可信计算基(Trusted Computing Base,TCB)界定发生了变化;物理资源的共享使恶意租户通过底层硬件环境对其他租户的虚拟机发起攻击成为可能. 此外,虚拟机的外包使用模式下,如何向用户证明虚拟机中执行内容符合用户要求也成为一个需要解决的问题. 下面,如图 3 所示,将从虚拟机执行验证、虚拟机监控与隔离、VMM 完整性保护等 3 个方面,对虚拟机的服务外包可信技术进行具体的分析与总结.

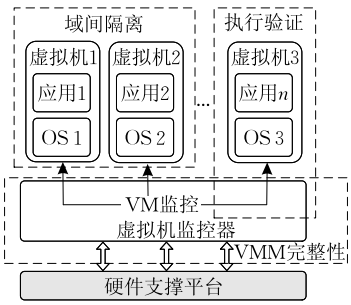

图 3 可信虚拟机外包主要技术

4.3.1 VM 执行验证

在虚拟机的外包服务模式中,虚拟机位于服务方,因此用户对于其具体操作在虚拟机上是否得到了正确执行、在其虚拟机上除了用户授权的服务外是否还存在其他服务等等问题都存在疑问,需要对虚拟机的执行过程进行验证. 针对这个问题,具体有两方面的研究:一类是利用可信计算技术与 VMM 相结合,向用户验证只有用户授权的应用在虚拟机上运行;另一种是记录虚拟机的行为,通过事后分析的手段来验证虚拟机的执行情况.

可信计算技术通过信任链为用户提供了远程验证功能,基于此项技术,Santos 等人[40]设计了可信云计算平台,通过 Terra 中的"封闭"式虚拟机,由可信的协调者利用 TVMM 的支持,为远程用户提供其虚拟机运行情况的执行验证信息. 随着可信计算技术的发展,McCune 等人[41]利用可信芯片的 Late Launch 支持,提出了代码可信执行架构 Flicker,该机制的目标是追求可信基 TCB 的最小化,通过 250 行代码即可完成系统执行的验证工作,并且同时可以向远程验证者提供代码执行情况的细粒度完整性度量.

Andreas 等人[42]提出了可记录的虚拟机(Accountable Virtual Machine,AVM)技术,将用户

所需要的服务置于 AVM 中执行，在服务过程中记录虚拟机的整个执行过程及通信消息. 审计人员通过对虚拟机的回放，可以判断虚拟机中运行的软件系统行为是否按照预期执行，为判断系统的可信执行提供证据. 由于虚拟机的回放过程中有可能涉及到用户的隐私，Richter 等人[43]对虚拟机回顾过程的隐私泄露问题进行了深入讨论，并提出了针对此问题的 VM 设计原则.

4.3.2　VM 安全监控与隔离

虚拟机环境允许在同一物理环境下运行多个虚拟机，与其他租户的物理共存(physical co-residency)成为潜在的危险. 为保障用户虚拟机的安全运行，服务提供商必须具有对单个 VM 进行监控的能力，同时，还必须保证运行在同一物理机上的虚拟机之间相互隔离.

在 VM 监控方面，可以通过将安全相关的工具集中放置在一个可信虚拟机中，通过底层 Hypervisor 的消息传递实现对其他非可信虚拟机的监控，这种做法带来了很大的运行环境切换开销. 为解决该问题，Payne 等人[44]提出一种利用虚拟化技术的安全监控体系结构，在非可信虚拟机中加入 Hook 函数，由 Hook 函数获取该虚拟机的执行情况，并将信息返回至安全监控器；而 Sharif 等人[45]设计了 Secure In-VM Monitor(SIM)，在 VM 内部实现监控工具，并利用硬件内存保护与硬件虚拟化技术来保护监控工具的执行空间，大大提高安全监控的执行效率；Azab 等人[46]则提出基于 Hypervisor 的虚拟机监控机制，着重解决了系统安全监控的经典问题 Time of Check to Time of Use (TOCTTOU)，对客户虚拟机的内存布局的变化以及使用保护等方面进行完整性度量.

此外，复旦大学的陈海波等人[47]利用嵌套虚拟化的技术来解决云计算多方租赁环境下的虚拟安全问题，提出了整体解决方案 cloudvisor. 该机制的主要方法是利用对虚拟化层的安全保护来实现对资源管理的隔离，并通过嵌套虚拟化技术，在商业的 VMM 之下引入小型的安全监控器对虚拟机进行保护.

4.3.3　VMM 完整性

作为虚拟机的管理中心，Hypervisor 在很多安全服务中起到了重要作用，上述对 VM 的安全监控等技术都是通过 Hypervisor 来完成. 如何保护 Hypervisor的完整性不被破坏，成为虚拟机安全的重要问题. 这类问题的解决方案主要依赖于使用独立的系统组件来对更高特权级别的软件完整性进行度量.

HyperGuard[48]与 HyperCheck[49]分别提出了 Hypervisor 完整性度量框架，依靠 CPU 的 SMM (System Management Mode)模式的辅助，在 Hypervisor之下建立新的特权软件层来维护上层软件的完整性；与 HyperGuard 的本地分析机制不同，HyperCheck 实现了远程的完整性信息分析，降低了分析工作对系统性能的影响. 具体工作时，HyperCheck在 BOIS 层利用 CPU 的 SMM 模式创建 CPU 以及内存寄存器的状态快照，记录机器的状态信息并将其传输至远程分析服务器，分析验证目标机的安全性.

与上述两者在 Hypervisor 之下添加一层可信监控的做法不同，HyperSentry[50]通过一个与 Hypervisor隔离的软件组件，实现对其运行时完整性进行度量，并且这种度量工作十分隐蔽，能够避免攻击者察觉而隐藏其攻击行为. HyperSentry 主要通过带外信道(如智能平台管理接口 IPMI)来触发度量行为，并利用 SMM 模式来保护其基本代码与关键数据.

4.3.4　分析与小结

虚拟机外包服务导致 VM 的执行难以验证，并且由于在硬件与操作系统中新添加了 VMM 层，VMM 的安全管理也成为必须解决的问题. 可信虚拟机外包服务的主要技术总结如表 3 所示.

表 3　可信虚拟机外包技术比较

安全问题	主要技术	用户信任预期		安全威胁来源			安全目标			
		完全	条件	一般	特权	共享资源	保密性	完整性	可控性	不可抵赖性
VM 执行验证	基于可信计算的验证执行		√		√				√	
	VM 行为记录与回放		√		√		√			√
VM 间安全监控与 VMM 完整性	VM 安全监控	√				√			√	
	Hypervisor 完整性度量	√		√				√		

在虚拟机外包服务中，虚拟机执行验证主要针对服务提供方可能没有真实地按照用户要求执行虚拟机的问题，通过可信计算芯片的验证执行或事后第三方追查的手段，来对虚拟机的执行行为进行控制；VM 间的安全隔离问题则主要针对多租户服务的特点，通过监控 VM 间的行为来保证 VM 间不互

相干扰.此外,作为系统结构中重要的一层,在解决VMM完整性问题上,通过不同的TCB划分,设计新的系统结构,引入安全验证模块来保护VMM的完整性.

目前虚拟机的安全隔离研究主要根据信息在系统中的逻辑流转路径进行分析,然后在关键点设计安全机制,对虚拟机的行为进行监控.然而,由于运行在同一物理设备上的虚拟机之间存在内存、cache等设备共享,攻击者可以通过硬件的记录特性等非直接的信息传输途径盗取信息.由于这类攻击行为不受系统安全逻辑的限制,造成防御上的难度.因此,针对虚拟机共享环境的旁路攻击与防御在后续研究中成为必须解决的问题.

5 未来研究趋势

通过分析总结可信云服务研究现状以及各个研究方向当前所存在的问题,可以将可信云服务未来的研究趋势概括为3个大的方向:首先,针对各类典型服务的可信性研究将进一步深化,在数据存储安全、计算外包验证以及系统安全等方面深入研究;其次,需要从云服务的总体结构上着眼研究,综合考虑各类云服务的一体化可信需求,建立面向多层服务间的服务监控体系;再次,由于当前情况下公有云的安全隐患阻碍了云服务的进一步扩展,业界与学术界期望能够从云结构上的改变来彻底提升云服务的可信性,提出了混合云的思想.因此,如何在新型云结构下建立可信云服务也成为了重要的研究趋势.下面,就对这些研究方向的新技术进行介绍.

5.1 典型服务外包可信新技术

首先,针对当前情况下,在数据外包、计算外包与虚拟机外包等典型服务的可信性研究方面存在的不足,进一步深入研究,具体的新型技术包括:

(1)数据隐私保护新技术

数据机密性是隐私保护的重要研究内容,一直以来,数据加密存储都是保证数据机密性的主流方法.但是,随着外包存储的数据应用范围的扩大,数据需要在云上进行多样性的计算,而各类用户对数据的访问行为也日趋复杂,因此,隐私保护研究的范围进一步扩大,新涌现的研究方向主要涉及动态数据隐私保护和用户访问行为的隐私保护两个方面:

用户的隐私数据可以细分为静态数据和动态数据两种.静态数据指用户的文档、资料等不参与计算的隐私信息;而动态数据则指需要参与计算的隐私信息.对静态数据的隐私保护主要通过加密来完成,将密文数据保存在云端即可防止数据隐私的泄露.而对于用户动态数据的隐私保护还没有一个彻底的解决方案.全同态加密为动态数据隐私保护提供了一种理论支持,但其在解决任意计算问题方面的实用性上还存在很大的差距.因此,这方面的研究主要还是针对特定的计算类型,应用全同态加密、Garbled电路等新型技术,研究代价可以被实际应用所接受的隐私保护机制.Nikolaenko等人[51]针对在推荐系统等领域应用广泛的岭回归算法,将同态加密与Yao garble电路相结合,保护用户数据隐私;在数据库方面,CryptDB[52]将存储的数据嵌套进多个加密层,每个都使用不同的密钥,并利用化简的全同态加密技术允许对加密数据进行简单的SQL操作.黄汝维等人[53]则设计了一个基于矩阵和向量运算的可计算加密方案,支持对加密字符串的模糊检索和对加密数值数据的加、减、乘、除4种算术运算.

除了数据隐私外,由于对数据的具体访问行为在云上完成,因此,用户对数据的访问行为也在一定程度上涉及用户的隐私.恶意攻击者可以通过对用户行为以及用户背景的总结来猜测数据的重要性、相关领域等信息.因此,对用户访问行为的隐私保护也逐渐受到研究者们的关注.Vimercati等人[54]将外包数据的隐私分为内容隐私、访问隐私以及模式隐私3类,并基于改进的B+树技术对访问隐私与模式隐私的保护进行了研究;而Lai等人[55]则在利用基于属性加密机制对数据进行访问控制时,研究对访问控制策略的隐私保护问题.

(2)计算外包验证新技术

云服务的外包服务模式,使得外包计算的验证方面成为近年研究热点,得到了安全顶级会议的持续关注.针对通用计算模式的验证主要依赖密码学方法完成,在此方面的研究主要有两个目标:追求更小的计算开销和适用更大的计算规模.Setty等人[56]对基于PCP的论证系统PEPPER进行改进,降低验证的网络与计算开销,设计能够支持不受限的、面向通用的、接近实际计算问题进行验证的PCP系统;Pinocchio方法[57]则基于密码学假设,为用户创建一个公开评价密钥,而计算方法则使用该密钥生成证据证明计算的正确性;Kreuter等人[58]则研究在恶意攻击模式下,如何对十亿级的门电路计算系统进行验证.

由于基于计算复杂性理论的验证方案计算开销巨大,并且目前的研究状态与大规模的实际应用还

有一定的距离，因此，还有一部分研究针对各种特定的问题，致力于研究实际可行的验证方案. 例如，Fiore 等人[59]通过数学变换对高阶多项式与矩阵乘进行验证. Vu 等人[60]则将上述基于密码学的验证与针对特定问题的验证方式相结合，提出了混合式的验证方式，根据具体的问题类型在密码学方法与非密码学方法之间切换.

(3)旁路攻击技术

云服务的资源共享特征为导致旁路攻击提供了便利. 旁路攻击是指利用物理实现等非直接传输途径的信息的攻击手段. 由于旁路攻击不是利用系统本身逻辑漏洞进行攻击，因此很难防御. 目前针对旁路攻击的研究主要从攻击手段以及防御机制两个方面双管齐下进行研究. Ristenpart 等人[61]在文章中分析了虚拟机方式带来的问题，通过在 Amazon EC2 上的实验，证明可以通过外包的 VM 获得云基础设施的内部结构、目标 VM 的位置以及同一物理机上的其他虚拟机分布等信息，并进一步通过一系列攻击来获得其他虚拟机的信息. Wu 等人[62]则针对虚拟 X86 平台研究基于旁路攻击的高带宽的攻击方式. 随着虚拟机环境下的旁路漏洞研究的进一步深入，针对旁路攻击的防御机制也有了初步成果，Kim 等人[63]提出了针对旁路攻击的系统级的防护技术 STEALTHMEM. 而 Zhang 等人[64]则对旁路攻击的思路加以正面利用，通过在 L2 cache 中分析 cache 的使用情况来探测是否存在共存的虚拟机，从而监控服务方是否履行了物理机独享的服务承诺.

5.2　云服务的全方位立体化监管

在云计算环境中，建立可控的云计算安全监管体系是云服务可信研究要解决的重要挑战[65]. 其中，面向多层服务的全方位监控体系与基于第三方的审计是实现安全监管的两个重要的研究方向.

未来云计算的发展方向将建立以云基础设施为基础、涵盖云平台服务与云应用服务等多个层次的立体化服务架构，各个层次的服务之间既彼此独立又相互依存. 因此，对于不同级别的服务，需要综合考虑服务在整个系统中的位置，研究层间、跨层的安全监控技术来保证系统的一体化安全. 例如，在系统安全层面，VMwatcher[66]针对虚拟机内省技术的语义鸿沟问题，提出了客户视图映射机制，为用户在虚拟机之外全面重建虚拟机内部视图；而 Srinivasan 等人[67]则使用了进程嫁接技术，实现对单独进程的执行监控. 在处理数据安全问题时，也将数据机密性保护与来自底层的安全监控技术相结合，例如，清华大学的侯清铧等人[68]提出将存储服务底层平台的 Daoli 安全虚拟监控系统与分布式文件系统相结合，利用安全虚拟监督系统来阻止传统攻击及来自云管理员的攻击. 而 Santos 等人[69]则利用商用 TPM 与基于属性加密技术，控制数据只有在授权的服务器上才可以解密，从而保护用户数据的机密性. 在针对服务行为的审计方面，当前主要使用基于密码学加密技术的验证方式，然而，随着云服务的进一步普及，针对云服务的监管体系将逐渐建立与完善，对云服务的第三方可信监管将逐渐取代用户自行验证. 例如在云存储服务中，为了保证数据的准确性与完整性，会引入第三方机构对数据进行审计，而服务商也必须为第三方机构的审计行为提供支持. 为此，Qian 等人[70]针对云计算环境提出了基于第三方的数据存储公开验证方案；而在 Cong 等人[71]的研究中，进一步研究在公开的第三方审计中，保护被审计数据的隐私不向审计方泄露.

5.3　基于混合云结构解决服务信任问题

公有云的安全威胁如何得到根本解决是产业界与学术界一直探讨的问题. 由于安全原因，当前情况下，并非所有的企业信息都能放置在公有云上. 在公有云的可信监管体制完备建立之前，业界与学术界都寻求一种从云计算结构上来解决问题的途径——将公有云和私有云两种服务方式结合，形成混合云. 在这种结构下，可以将有安全需求的计算与数据保留在私有云进行，其余公开业务则由公有云托管. 因此，利用混合云的架构来解决云服务的安全可信问题成为一种未来的研究趋势. 在人类基因序列匹配的计算中，Chen 等人[72]研究如何通过混合云结构来完成保护用户隐私的基因比对，将用户隐私的基因组分析保留在私有云中进行，而将大量的对参考基因组的分析则外包至云上进行. 在 Sedic[73]中，设计了适应混合云架构的 MapReduce 机制，根据用户数据的安全级别自动划分任务，并在混合云上进行资源调度. 而 Wang 等人[74]则对混合云架构下的 MapReduce 计算结果验证进行研究，提出了跨混合云的 MapReduce 系统 CCMR(Cross Cloud MapReduce)，通过中间结果分片等技术来减小混合云间的验证数据传输开销.

6　结束语

随着云计算技术进一步成熟，云服务将逐渐成为主流的互联网服务模式，而随之而来的云服务可

信性问题也将成为未来在信息安全学术界与产业界的关注焦点.本文首先深入剖析了云计算的特点与存在的安全威胁,提出了可信云服务的定义,并从用户信任预期、安全威胁来源以及技术的安全目标3个方面对可信云服务的研究工作进行分类;然后对作为当前成为研究焦点的数据存储外包、计算外包以及虚拟机外包等3类云服务的可信性研究关键技术进行了分析总结;最后探讨了可信云服务的未来研究趋势,为研究人员从概念、关键技术到未来趋势等方面深度把握可信云服务的最新研究动态提供了全方位的参考.

参 考 文 献

[1] Armbrust M, Fox A, Griffith R, et al. Above the clouds: A Berkeley view of cloud computing. EECS Department, University of California, Berkeley: Technical Report UCB/EECS-2009-28, 2009

[2] Chawla V, Sogani P. Cloud computing—The future//Proceedings of the International Conference on High Performance Architecture and Grid Computing. Chandigarh, India, 2011: 113-118

[3] Perlman R. File system design with assured delete//Proceedings of the 3rd IEEE International Security in Storage Workshop. San Francisco, USA, 2005: 83-88

[4] Geambasu R, Kohno T, Levy A A, Levy H M. Vanish: Increasing data privacy with self-destructing data//Proceedings of the 18th Conference on USENIX Security Symposium. Montreal, Canada, 2009: 299-316

[5] Yang T, Lui J C S, Perlman R. FADE: Secure overlay cloud storage with file assured deletion//Proceedings of the 6th International ICST Conference on Security and Privacy in Communication Networks. Singapore, 2010: 380-397

[6] Wang Li-Na, Ren Zheng-Wei, Yu Rong-Wei, et al. A data assured deletion approach adapted for cloud storage. Acta Electronica Sinica, 2012, 40(2): 266-272(in Chinese)
(王丽娜,任正伟,余荣威等. 一种适于云存储的数据确定性删除方法. 电子学报, 2012, 40(2): 266-272)

[7] Juels A, Burton S, Kaliski J. PORs: Proofs of retrievability for large files//Proceedings of the 14th ACM Conference on Computer and Communications Security. Alexandria, USA, 2007: 584-597

[8] Shacham H, Waters B. Compact proofs of retrievability//Proceedings of the 14th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology. Melbourne, Australia, 2008: 90-107

[9] Dodis Y, Vadhan S, Wichs D. Proofs of retrievability via hardness amplification//Proceedings of the 6th Theory of Cryptography Conference on Theory of Cryptography. San Francisco, USA, 2009: 109-127

[10] Ateniese G, Burns R, Curtmola R, et al. Provable data possession at untrusted stores//Proceedings of the 14th ACM Conference on Computer and Communications Security. Alexandria, USA, 2007: 598-609

[11] Erway C K A, Papamanthou C, Tamassia R. Dynamic provable data possession//Proceedings of the 16th ACM Conference on Computer and Communications Security. Chicago, USA, 2009: 213-222

[12] Curtmola R, Khan O, Burns R, Ateniese G. MR-PDP: Multiple-replica provable data possession//Proceedings of the 28th International Conference on Distributed Computing Systems. Beijing, China, 2008: 411-420

[13] Li M, Li SY, Ren K, Lou W. Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings//Proceedings of the 6th International ICST Conference on Security and Privacy in Communication Networks. Singapore, 2010: 89-106

[14] Goyal V, Pandey O, Sahai A, Waters B. Attribute-based encryption for fine-grained access control of encrypted data//Proceedings of the 13th ACM Conference on Computer and Communications Security. Alexandria, USA, 2006: 89-98

[15] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption//Proceedings of the 2007 IEEE Symposium on Security and Privacy. Oakland, USA, 2007: 321-334

[16] Yu S, Wang C, Ren K, Lou W. Achieving secure, scalable, and fine-grained data access control in cloud computing//Proceedings of the 29th Conference on Information Communications. San Diego, USA, 2010: 534-542

[17] Sun Guo-Zi, Dong Yu, Li Yun. CP-ABE based data access control for cloud storage. Journal of Communications, 2011, 32(7): 146-152(in Chinese)
(孙国梓,董宇,李云. 基于CP-ABE算法的云存储数据访问控制. 通信学报, 2011, 32(7): 146-152)

[18] Hong Cheng, Zhang Min, Feng Deng-Guo. Achieving efficient dynamic cryptographic access control in cloud storage. Journal of Communications, 2011, 32(7): 125-132(in Chinese)
(洪澄,张敏,冯登国. 面向云存储的高效动态密文访问控制方法. 通信学报, 2011, 32(7): 125-132)

[19] Boneh D, Waters B. Conjunctive, subset, and range queries on encrypted data//Proceedings of the 4th Conference on Theory of Cryptography. Amsterdam, The Netherlands, 2007: 535-554

[20] Katz J, Sahai A, Waters B. Predicate encryption supporting disjunctions, polynomial equations, and inner products//Proceedings of the Theory and Applications of Cryptographic Techniques 27th Annual International Conference on Advances in Cryptology. Istanbul, Turkey, 2008: 146-162

[21] Wang C, Ren K, Yu S, Urs K M R. Achieving usable and privacy-assured similarity search over outsourced cloud data//Proceedings of the IEEE INFOCOM. Orlando, USA, 2012: 451-459

[22] Zhu B, Zhu B, Ren K. PEKSrand: Providing predicate privacy in public-key encryption with keyword search//Proceedings of the 2011 IEEE International Conference on Communications. Kyoto, Japan, 2011: 1-6

[23] Cao N, Wang C, Li M, et al. Privacy-preserving multi-keyword ranked search over encrypted cloud data//Proceedings of the IEEE INFOCOM. Shanghai, China, 2011: 829-837

[24] Li M, Yu S, Cao N, Lou W. Authorized private keyword search over encrypted data in cloud computing//Proceedings of the 2011 International Conference on Distributed Computing Systems. Minneapolis, USA, 2011: 383-392

[25] Cao N, Yang Z, Wang C, et al. Privacy-preserving query over encrypted graph-structured data in cloud computing//Proceedings of the 2011 31st International Conference on Distributed Computing Systems. Minneapolis, USA, 2011: 393-402

[26] Goldwasser S, Kalai Y T, Rothblum G N. Delegating computation: Interactive proofs for muggles//Proceedings of the 40th Annual ACM Symposium on Theory of Computing. Victoria, Canada, 2008: 113-122

[27] Setty S, Mcpherson R, Blumberg A, Walfish M. Making argument systems for outsourced computation practical (sometimes)//Proceedings of the NDSS Symposium. Bloomington, USA, 2012: 1-20

[28] Cormode G, Thaler J, Yi K. Verifying computations with streaming interactive proofs. Proceedings of the VLDB Endowment, 2011, 5(1): 25-36

[29] Gentry C. A Fully Homomorphic Encryption Scheme[Ph. D. dissertation]. Stanford University, Stanford, USA, 2009

[30] Chung K-M, Kalai Y, Vadhan S. Improved delegation of computation using fully homomorphic encryption//Proceedings of the 30th Annual Conference on Advances in Cryptology. Santa Barbara, USA, 2010: 483-501

[31] Gennaro R, Gentry C, Parno B. Non-interactive verifiable computing: Outsourcing computation to untrusted workers//Proceedings of the 30th Annual Conference on Advances in cryptology. Santa Barbara, USA, 2010: 465-482

[32] Atallah M J, Frikken K B. Securely outsourcing linear algebra computations//Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. Beijing, China, 2010: 48-59

[33] Wang C, Ren K, Wang J, Wang Q. Harnessing the cloud for securely outsourcing large-scale systems of linear equations. IEEE Transactions on Parallel and Distributed Systems, 2013, 24(6): 1172-1181

[34] Wang C, Ren K, Wang J. Secure and practical outsourcing of linear programming in cloud computing//Proceedings of the IEEE INFOCOM. Shanghai, China, 2011: 820-828

[35] Wei W, Du J, Yu T, Gu X. SecureMR: A service integrity assurance framework for MapReduce//Proceedings of the 2009 Annual Computer Security Applications Conference. Honolulu, USA, 2009: 73-82

[36] Wang Y, Wei J. VIAF: Verification-based integrity assurance framework for MapReduce//Proceedings of the IEEE CLOUD. Washington DC, USA, 2011: 300-307

[37] Xiao Z, Xiao Y. Accountable MapReduce in cloud computing//Proceedings of the IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). Shanghai, China, 2011: 1082-1087

[38] Huang C, Zhu S, Wu D. Towards trusted services: Result verification schemes for MapReduce//Proceedings of the 2012 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing. Ottawa, Canada, 2012: 41-48

[39] Roy I, Setty S T V, Kilzer A, et al. Airavat: Security and privacy for MapReduce//Proceedings of the 7th USENIX Conference on Networked Systems Design and Implementation. San Jose, USA, 2010: 20-20

[40] Santos N, Gummadi K P, Rodrigues R. Towards trusted cloud computing//Proceedings of the 2009 Conference on Hot Topics in Cloud Computing. San Diego, USA, 2009: 1-5

[41] McCune J M, Parno B J, Perrig A, et al. Flicker: An execution infrastructure for TCB minimization//Proceedings of the 3rd ACM SIGOPS/EuroSys European Conference on Computer Systems. Glasgow, Scotland UK, 2008: 315-328

[42] Haeberlen A, Aditya P, Rodrigues R, Druschel P. Accountable virtual machines//Proceedings of the 9th USENIX Conference on Operating Systems Design and Implementation. Vancouver, Canada, 2010: 1-16

[43] Richter W, Ammons G, Harkes J, et al. Privacy-sensitive VM retrospection//Proceedings of the 3rd USENIX Conference on Hot Topics in Cloud Computing. Portland, OR, 2011: 1-6

[44] Payne B D, Carbone M, Sharif M, Lee W. Lares: An architecture for secure active monitoring using virtualization//Proceedings of the 2008 IEEE Symposium on Security and Privacy. Oakland, USA, 2008: 233-247

[45] Sharif M I, Lee W, Cui W, Lanzi A. Secure in-VM monitoring using hardware virtualization//Proceedings of the 16th ACM Conference on Computer and Communications Security. Chicago, USA, 2009: 477-487

[46] Azab A M, Ning P, Sezer E C, Zhang X. HIMA: A hypervisor-based integrity measurement agent//Proceedings of the 2009 Annual Computer Security Applications Conference. Honolulu, USA, 2009: 461-470

[47] Zhang F, Chen J, Chen H, Zang B. CloudVisor: Retrofitting protection of virtual machines in multi-tenant cloud with nested virtualization//Proceedings of the 23rd ACM Symposium on Operating Systems Principles. Cascais, Portugal, 2011: 203-216

[48] Wojtczuk R, Rutkowska J. Xen 0wning trilogy. Caesars Palace, USA: Invisible Things Lab, Black Hat, 2008

[49] Wang J, Stavrou A, Ghosh A. HyperCheck: A hardware-assisted integrity monitor//Proceedings of the 13th International Conference on Recent Advances in Intrusion detection. Ottawa, Canada, 2010: 158-177

[50] Azab A M, Ning P, Wang Z, et al. Hypersentry: Enabling stealthy in-context measurement of hypervisor integrity// Proceedings of the 17th ACM Conference on Computer and Communications Security. Chicago, USA, 2010: 38-49

[51] Nikolaenko V, Weinsberg U, Ioannidis S, et al. Privacy-preserving ridge regression on hundreds of millions of records //Proceedings of the 2013 IEEE Symposium on Security and Privacy. Berkeley, USA, 2013: 334-348

[52] Raluca A P, Catherine M S R, Nickolai Z, Hari B. CryptDB: Protecting confidentiality with encrypted query processing// Proceedings of the 23th ACM Symposium on Operating Systems Principles. New York, USA, 2011: 85-100

[53] Huang Ru-Wei, Gui Xiao-Lin, Yu Si, Zhuang Wei. Privacy-preserving computable encryption scheme of cloud computing. Chinese Journal of Computers, 2011, 34(12): 2391-2402(in Chinese)
(黄汝维，桂小林，余思，庄威. 云环境中支持隐私保护的可计算加密方法. 计算机学报，2011，34(12)：2391-2402)

[54] Vimercati S D C D, Foresti S, Paraboschi S, et al. Efficient and private access to outsourced data//Proceedings of the 31st International Conference on Distributed Computing Systems. Minneapolis, USA, 2011: 710-719

[55] Lai J, Deng R, Li Y. Fully secure cipertext-policy hiding cp-abe//Proceedings of the 7th International Conference of Information Security Practice and Experience. Guangzhou, China, 2011: 24-39

[56] Setty S, Vu V, Panpalia N, et al. Taking proof-based verified computation a few steps closer to practicality// Proceedings of the 21st USENIX Conference on Security Symposium. Bellevue, USA, 2012: 12-12

[57] Parno B, Howell J, Gentry C, Raykova M. Pinocchio: Nearly practical verifiable computation//Proceedings of the 2013 IEEE Symposium on Security and Privacy. Berkeley, USA, 2013: 238-252

[58] Kreuter B, Shelat A, Shen C-H. Billion-gate secure computation with malicious adversaries//Proceedings of the 21st USENIX Conference on Security Symposium. Bellevue, USA, 2012: 14-14

[59] Fiore D, Gennaro R. Publicly verifiable delegation of large polynomials and matrix computations, with applications// Proceedings of the 2012 ACM Conference on Computer and Communications Security. Raleigh, USA, 2012: 501-512

[60] Vu V, Setty S, Blumberg A J, Walfish M. A hybrid architecture for interactive verifiable computation//Proceedings of the 2013 IEEE Symposium on Security and Privacy. Berkeley, USA, 2013: 223-237

[61] Ristenpart T, Tromer E, Shacham H, Savage S. Hey, you, get off of my cloud: Exploring information leakage in 3rd-party compute clouds//Proceedings of the 16th ACM Conference on Computer and Communications Security. Chicago, USA, 2009: 199-212

[62] Wu Z, Xu Z, Wang H. Whispers in the hyper-space: High-speed covert channel attacks in the cloud//Proceedings of the 21st USENIX Conference on Security Symposium. Bellevue, USA, 2012: 9-9

[63] Kim T, Peinado M, Mainar-Ruiz G. StealthMem: System-level protection against cache-based side channel attacks in the cloud//Proceedings of the 21st USENIX Conference on Security Symposium. Bellevue, USA, 2012: 11-11

[64] Zhang Y, Juels A, Oprea A, Reiter M K. HomeAlone: Co-residency detection in the cloud via side-channel analysis// Proceedings of the 2011 IEEE Symposium on Security and Privacy. Oakland, USA, 2011: 313-328

[65] Feng Deng-Guo, Zhang Min, Zhang Yan, Xu Zhen. Study on cloud computing security. Journal of Software, 2011, 22(1): 71-83(in Chinese)
(冯登国，张敏，张妍，徐震. 云计算安全研究. 软件学报，2011，22(1)：71-83)

[66] Jiang X, Wang X, Xu D. Stealthy malware detection through VMM-based "Out-of-the-box" Semantic view reconstruction// Proceedings of the 14th ACM Conference on Computer and Communications Security. Alexandria, USA, 2007: 128-138

[67] Srinivasan D, Wang Z, Jiang X, Xu D. Process out-grafting: An efficient "Out-of-VM" Approach for fine-grained process execution monitoring//Proceedings of the 18th ACM Conference on Computer and Communications Security. Chicago, USA, 2011: 363-374

[68] Hou Qing-Hua, Wu Yong-Wei, Zheng Wei-Min, Yang Guang-Wen. A method on protection of user data privacy in cloud storage platform. Journal of Computer Research and Development, 2011, 48(7): 1146-1154(in Chinese)
(侯清铧，武永卫，郑纬民，杨广文. 一种保护云存储平台上用户数据私密性的方法. 计算机研究与发展，2011，48(7)：1146-1154)

[69] Santos N, Rodrigues R, Gummadi K P, Saroiu S. Policy-sealed data: A new abstraction for building trusted cloud services//Proceedings of the 21st USENIX Conference on Security Symposium. Bellevue, USA, 2012: 10-10

[70] Wang Qian, Wang Cong, Li Jin, et al. Enabling public verifiability and data dynamics for storage security in cloud computing. IEEE Transactions on Parallel and Distributed Systems, 2011, 22(5): 847-859

[71] Wang C, Chow S S M, Wang Q, et al. Privacy-preserving public auditing for secure cloud storage. IEEE Transactions on Computers, 2013, 62(2): 362-375

[72] Chen Y, Peng B, Wang X, Tang H. Large-scale privacy-preserving mapping of human genomic sequences on hybrid clouds//Proceedings of the 2012 NDSS Symposium. Bloomington, USA, 2012

[73] Zhang K, Zhou X, Chen Y, et al. Sedic: Privacy-aware data intensive computing on hybrid clouds//Proceedings of the 18th ACM conference on Computer and Communications security. Chicago, USA, 2011: 515-526

[74] Wang Y, Wei J, Srivatsa M. Result integrity check for MapReduce computation on hybrid clouds//Proceedings of the 2013 IEEE 6th International Conference on Cloud Computing. Santa Clara Marriott, USA, 2013: 847-854

DING Yan, born in 1977, Ph. D., assistant professor. Her current research interests include information security, operating system and distributed computing.

WANG Huai-Min, born in 1962, Ph. D., professor, Ph. D. supervisor. His research interests include distributed computing, information security and software engineering.

SHI Pei-Chang, born in 1981, Ph.D., assistant professor. His research interests include information security, cloud computing and content distribution networks.

WU Qing-Bo, born in 1969, Ph. D., professor. His research interests include basic software, operating system.

DAI Hua-Dong, born in 1975, Ph. D., professor. His research interests include basic software, operating system.

FU Hong-Yi, born in 1978, Ph. D., engineer. His research interests include high performance computing, parallel computing, parallel compiling and fault tolerance.

Background

Cloud computing is an Internet-based computing paradigm, which provides shared resources to users on-demand as public utility. Cloud service is an emerging network service pattern based on the platform of cloud computing. As the cloud service provides remarkable convenience to the users, issues arise with its outsourcing service mode; that is, the control of resources and processing shifts from the user to the cloud service provider, which will result in uncontrollable service processing. And at the same time, the complicated implementation and source sharing mode of the cloud platform also bring new security challenges. How to achieve trusted cloud service becomes the hotspot of research.

In this paper, we make analysis on the security challenges of cloud computing, give the definition of trusted cloud service and the taxonomies of the techniques on this topic. Based on the survey of three outsourcing services which gained much more attention currently, a set of research directions that we believe to be the most important ones in the near future are provided. We hope that all of this can help and inspire the researchers.

This work is supported by the National Grand Fundamental Research 973 Program of China under Grant No. 2011CB302600: "Basic Research on Effective and Trustworthy Internet-Based Virtual Computing Environment (iVCE)", whose purpose is to design basic models and mechanisms for effective and trustworthy virtual computing environment. Many achievements have been made by our research team: A theory system of Internet-Based Virtual Computing Environment has been built, nearly 600 papers were published and a number of awards such as the prize of National Science & Technology Improvement were obtained. This paper is focus on the current research techniques on the trusted cloud service, which is helpful for concluding the state of current research and forecasting the upcoming research spots. All of these lay the foundation of our subsequent research.

This work is also supported by the National Natural Science Foundation of China under Grant No. 61161160565: "Research on the Component-Based Design, Online Evaluation and Runtime Optimization of Trustworthy Cloud Computing", whose purpose is to tackle the major challenges of building trustworthy cloud computing platforms.